THE TECHNOLOGY PROVIDER

TECH& SNACK

FortiOS 7.4 – What's New?

30.Juni in Emmen

WER WIR SIND

Andreas (Andi) Tischer

Channel PreSales Engineer
Fortinet Schweiz

Martin (Tinu) Ruesch

Tech. Consultant Security
ALSO Schweiz

Cvijetin (Chris) Tanasic

Tech. Consultant Security
ALSO Schweiz

Guido Handel

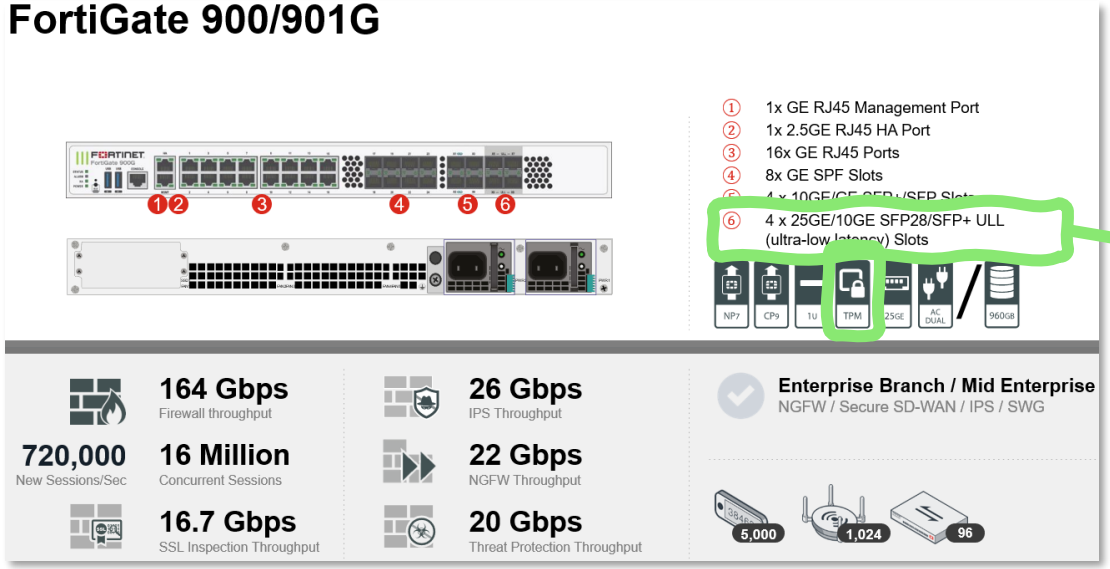
OT Security System Engineer
Fortinet Schweiz

WAS EUCH HEUTE ERWARTET

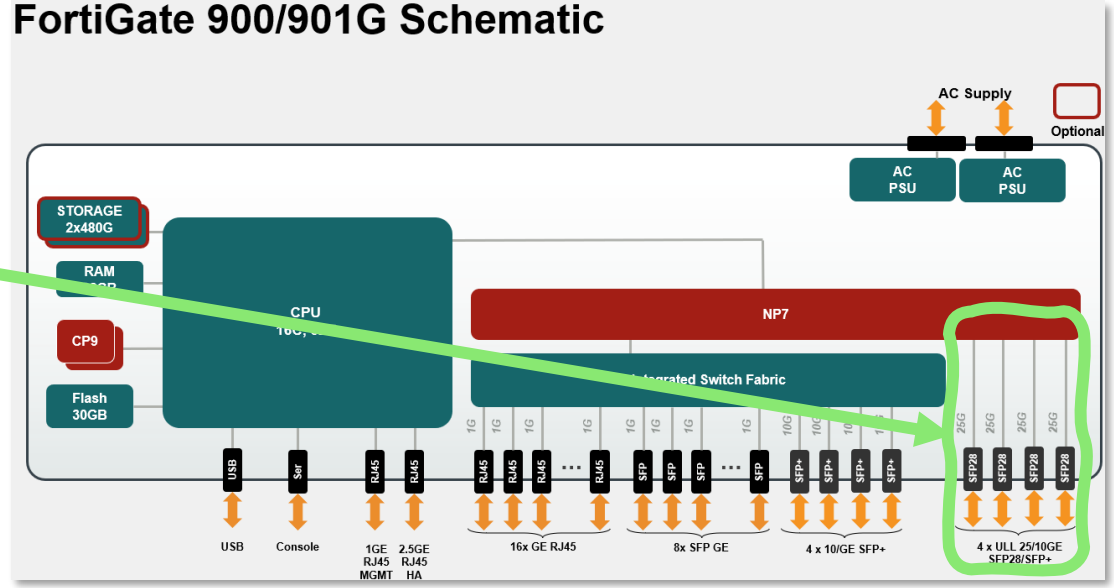
- Neues Produkt – FortiGate 900/901G
- Hinweis FortiOS 6.2
- Was gibt es Neues im FortiOS 7.4?
- Agora Community
- Fragen

NEUES PRODUKT – FORTIGATE 900/901G

FortiGate 900/901G



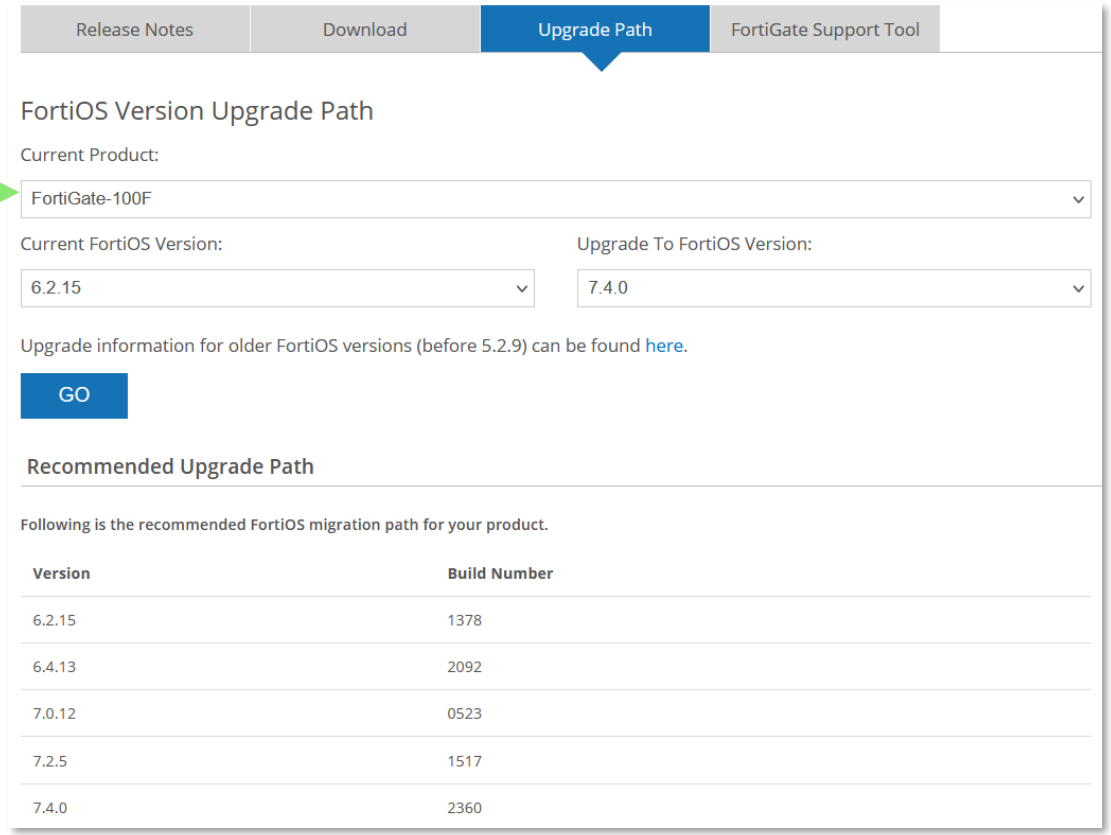
FortiGate 900/901G Schematic



FORTIOS 6.2 – GEHT END-OF-SUPPORT (28.9.23)

- FortiOS wird Ende September 2023 **E**nd **o**f **S**upport gehen (EoS)
- Upgraden auf eine supportete Version
- Upgrade Pfad beachten!
- Infos in unserem WIKI:

Software Version	Release Date (GA)	End of Engineering Support Date (EOES)	End of Support Date (EOS)
6.0	29.03.2018	29.03.2021	**29.09.2022**
6.2	28.03.2019	28.03.2022	28.09.2023 ⚠
6.4	31.03.2020	31.03.2023	30.09.2024
7.0	30.03.2021	30.03.2024	30.09.2025
7.2	31.03.2022	31.032025	30.09.2026
7.4	11.05.2023	11.05.2026	11.11.2027



- Offizieller Lifecycle:
  https://support.fortinet.com/Information/ProductLifeCycle.aspx

WAS GIBT ES NEUES IM FORTIOS 7.4?

PLATFORM SUPPORT – FORTIOS 7.4.0

	7.0.12	7.2.5	7.4
FG/FWF-60E/80E/90E	●	●	●
FG/FWF-40F Series	●	●	●
FG/FWF-60F Series	●	●	●
FG-70F Series	●	●	●
FG-80E Series	●	●	●
FG/FWF-80F Series	●	●	●
FG-100/101E Series	●	●	no
FG-100F Series	●	●	●
FG-200/201E	●	●	●
FG-200F	●	●	●
FG-400F/600F Series	●	●	●
FG-400E/600E Series	●	●	●
FG-900G Series	*	??	??
FG-1500D Series	●	●	no

	7.0.12	7.2.5	7.4
FG-1100E Series	●	●	●
FG-1000F Series	#	●	7.4.1
FG-1800F Series	●	●	●
FG-2200E, 3300E Series	●	●	●
FG-2000E, 2500E	●	●	●
FG-2600F Series	●	●	●
FG-3000F Series	●	●	Geplant
FG 3200F Series	#	Geplant	7.4.x
FG-3400E/3600E	●	●	●
FG-3500F Series	●	●	●
FG-3700F Series	#	Geplant	7.4.x
FG-4200/4400F Series	●	●	●
FG-4800 Series	#	7.2.6	7.4.1

* es existiert ein Special Brand im 7.0.10 Build 6607

Special Brand vorhanden (siehe Release Notes)

PLATFORM SUPPORT – FORTIOS 7.4.0

Supported models

FortiOS 7.4.0 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-70F, FG-71F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100F, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3000F, FG-3001F, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1, FG-6000F, FG-7000E, FG-7000F
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G
FortiFirewall	FFW-3980E, FFW-VM64, FFW-VM64-KVM
FortiGate VM	FG-ARM64-AWS, FG-ARM64-AZURE, FG-ARM64-GCP, FG-ARM64-KVM, FG-ARM64-OCI, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-XEN

FortiGate 6000 and 7000 support

FortiOS 7.4.0 supports the following FG-6000F, FG-7000E, and FG-7000F models:

The hardware models listed below do not support FortiOS version 7.4:

FortiGate 100E, 101E, 100EF, 1500D, 1500DT. Access to Fortinet Customer Services for support on 7.2 is available for these hardware models until they reach their hardware End-of-Support date.

FORTI AP KOMPATIBILITÄT

- Folgende APs werden vom FortiOS 7.4 unterstützt:
  - FortiAP E-Serie
  - FortiAP F-Serie
  - FortiAP G-Serie
  - APs müssen mindestens FortiOS 7.2.2 installiert haben!

- Modelle der **Serie B, C** und **D** werden **nicht** mehr vom FortiOS 7.4.0 unterstützt

FortiOS 7.4.x compatibility

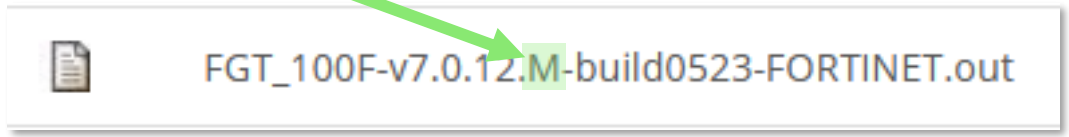
FortiAP	FortiOS Versions 7.4.0
Wi-Fi 6 Models	
FAP-23JF	7.4.0
FAP-231F	7.4.0
FAP-234F	7.4.0
FAP-431F	7.4.0
FAP-432F	7.4.0
FAP-433F	7.4.0
FAP-831F	7.4.0
Wi-Fi 6E Models	
FAP-231G	7.4.0
FAP-233G	7.4.0
FAP-431G	7.4.0
FAP-433G	7.4.0

FortiGates running FortiOS version 7.4.0 do not support legacy FortiAP models (B, C and D series).

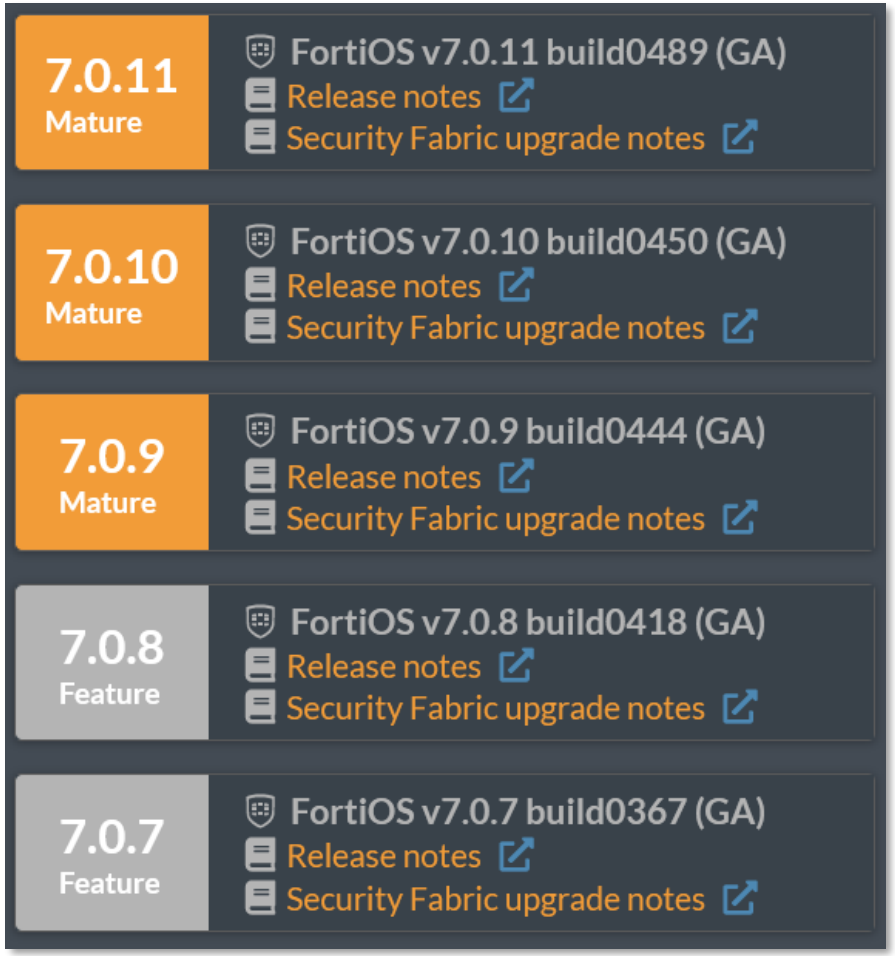
BEZEICHNUNG FEATURE / MATURE

- **Feature** : Patch enthält neue Features und Bugfixes. Wird durch ein **F** markiert:

- **Mature** : Patch enthält Bugfixes, keine neuen Features werden hinzugefügt. Wird durch ein **M** markiert.



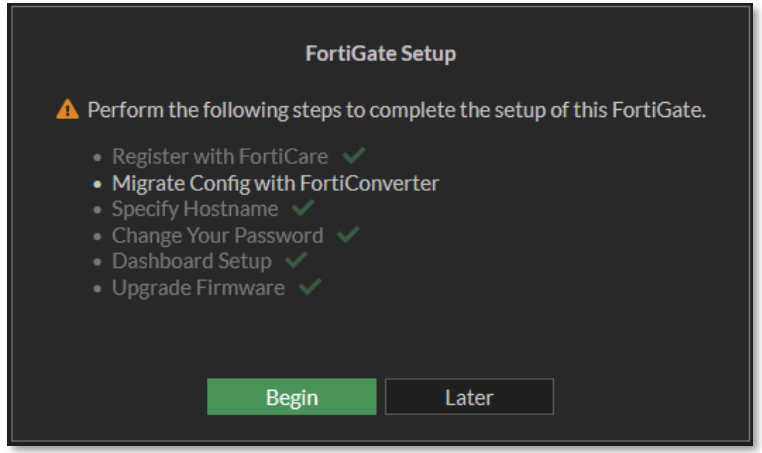
- Für produktive Systeme empfehlen wir ausschliesslich **Mature Patches** zu installieren



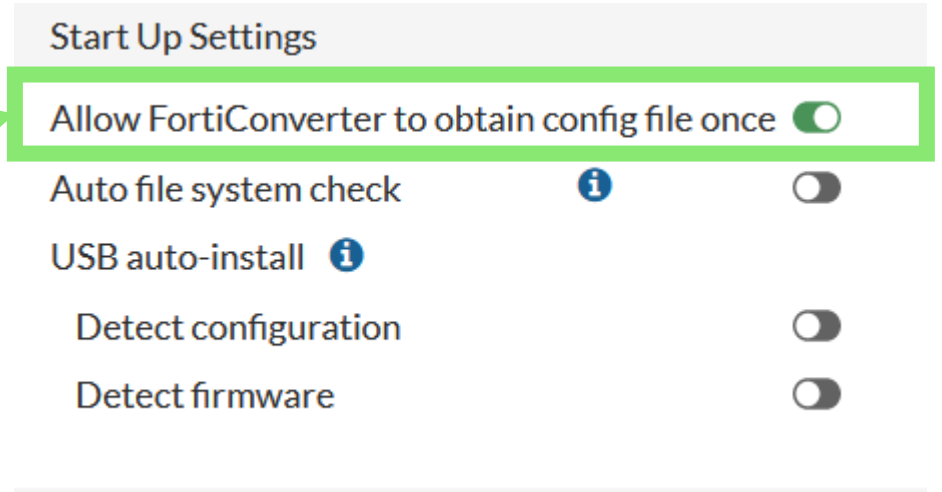
NEUES IM WEBGUI – DASHBOARD – LIVE DEMO

WEBGUI: INTEGRIERTER FORTI CONVERTER SERVICE

- Kostenpflichtiger Service
  - Im Enterprise Bundle inkludiert
  - A la Carte Service: FC-10-0060F-189-02-DD
    0060F Zielsystem (siehe Datenblatt)
  - Lizenz muss auf dem Zielsystem gelöst sein

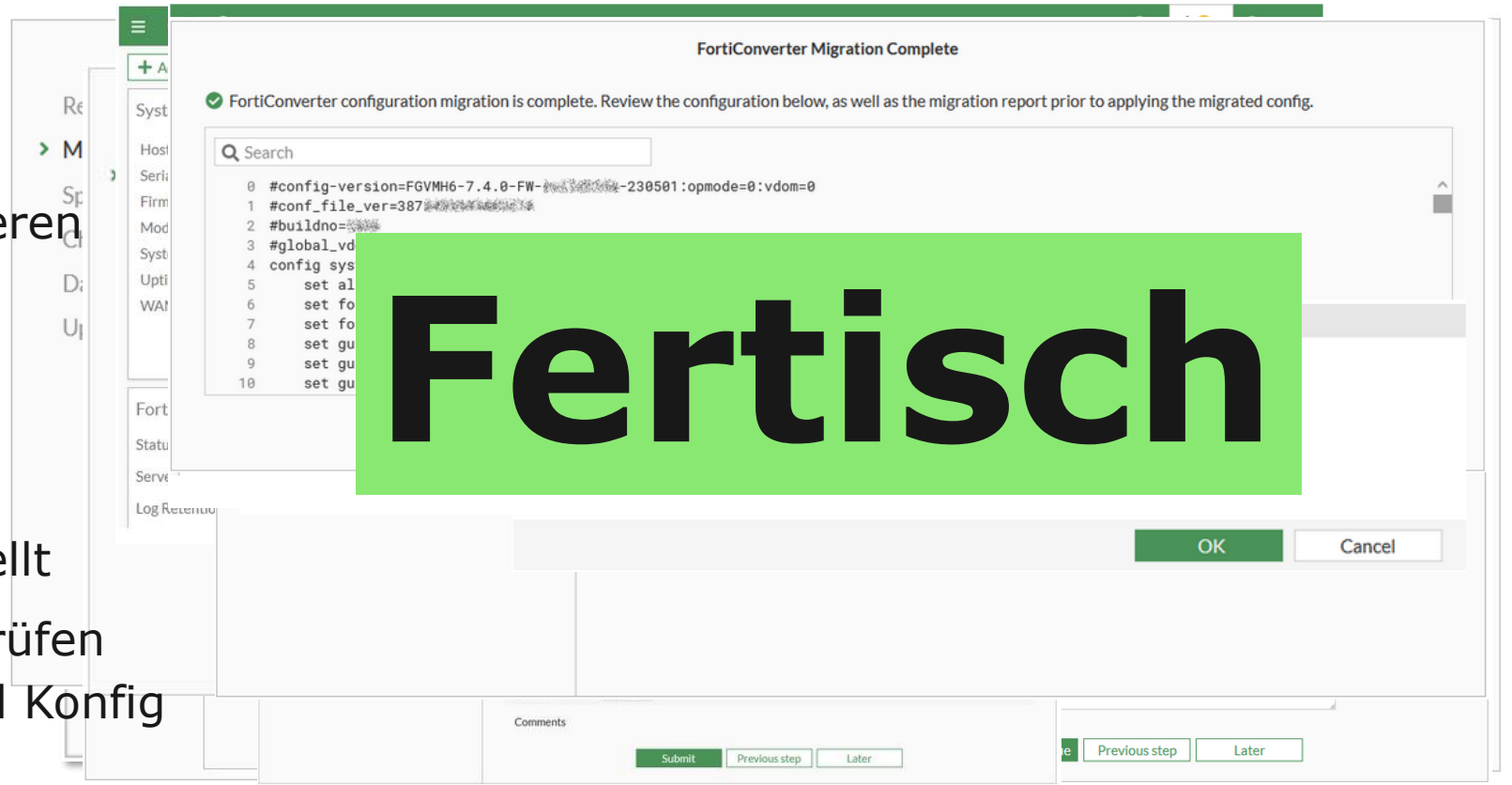


- Konvertieren mit Backupfile der Source FortiGate
- Konvertieren direkt von der Source FortiGate mit eingeschalteter Option



FORTI CONVERTER IM ZEITRAFFER

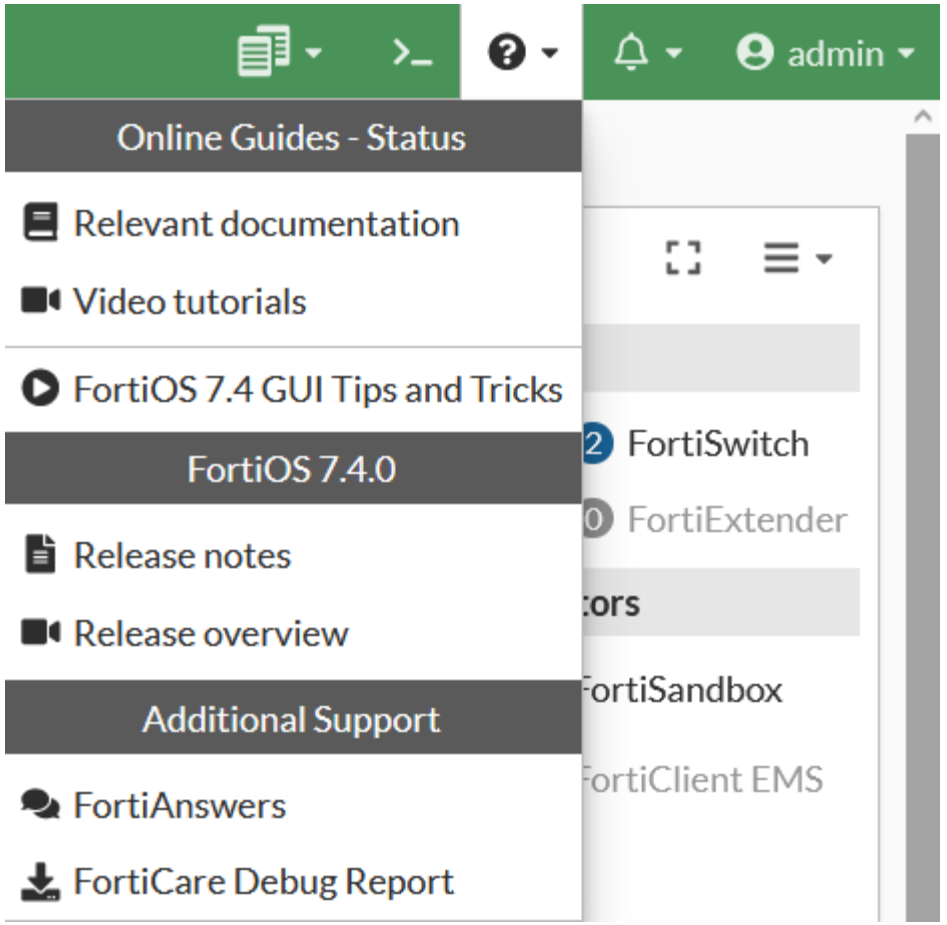
- ☑ Mit Begin Wizard starten
- ☑ Source der Konfig definieren
- ☑ Konfiguration wird hochgeladen
- ☑ Interface Mappings definieren
- ☑ Eventuell MGMT Interface definieren
- ☑ Kontakt Informationen angeben
- ☑ Einstellungen überprüfen
- ☑ Bestätigen und Prozess starten
- ☑ Ticket erstellt mit Ticketnummer
- ☑ Bestätigungs E-Mail wird zugestellt
- ☑ Aktuellen Status im Menu überprüfen
- ☑ Wenn komplett, kann Report und Konfig File heruntergeladen werden
- ☑ Bestätigungs E-Mail sobald Konvertierung fertig ist
- ☑ Notifikation im Menu → Download des Reports und der Konfig →Konfig File einspielen



WEBGUI: ZUSÄTZLICHE UNTERSTÜTZUNG

- Überarbeitetes Hilfe Menu

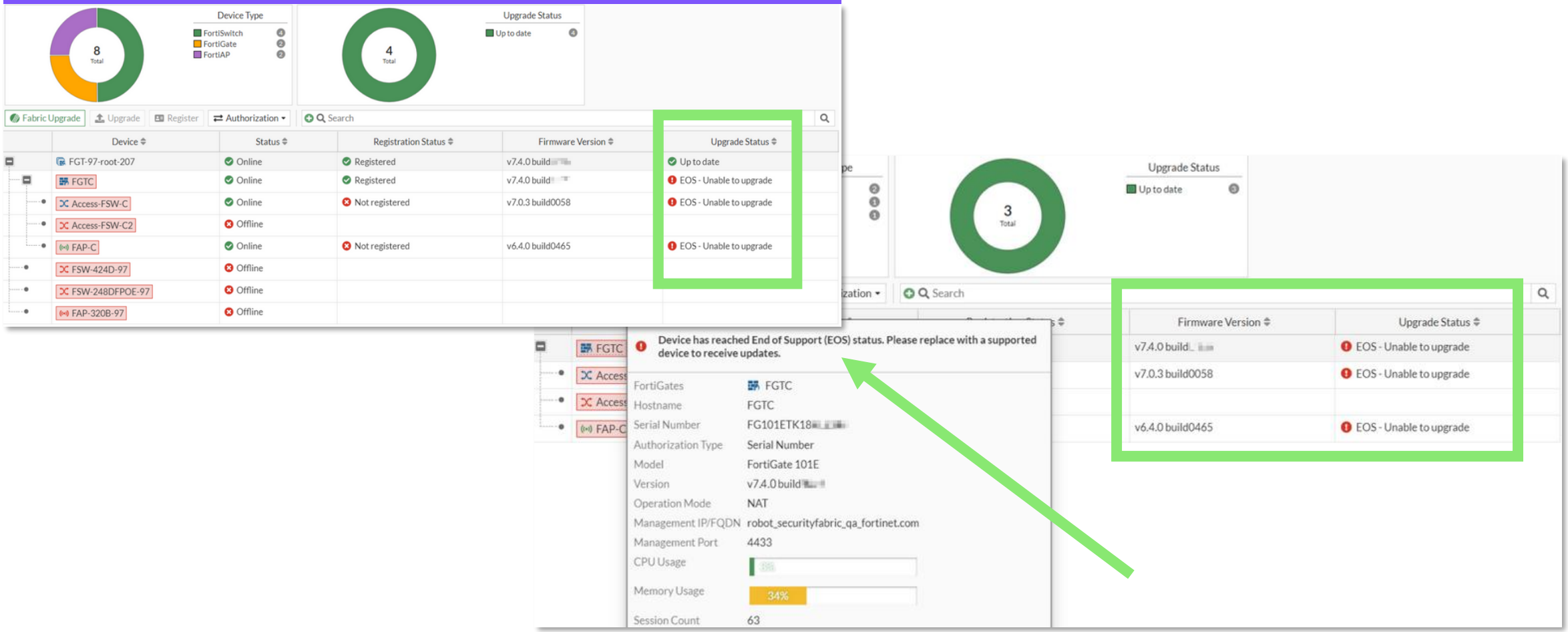
- Direkter Zugriff zu Release Notes
- Direkter Zugriff zu FortiAnswers
- TAC Report für L1 Tickets
- Kommando Palette `ctrl+p` (mac: `cmd+p`)



NEUE FEATURES BEIM UPDATEN

WARNUNG FÜR HARDWARE MIT EOS DATUM

Menu: System → Firmware & Registration



AUTOMATISCHE UPDATES

- Führt automatisch einen Software Update aus
  (Parameter können in der CLI konfiguriert werden)
- Führt Updates nur im selben GA Range aus
  - Update : **7.4.0** → **7.4.1** (Update wird ausgeführt)
  - Update : **7.4.5** → **7.6.0** (Update wird nicht ausgeführt, da neuer GA Release)
- Nach dem Update wird ein E-Mail an die FortiCloud Account Adresse gesendet

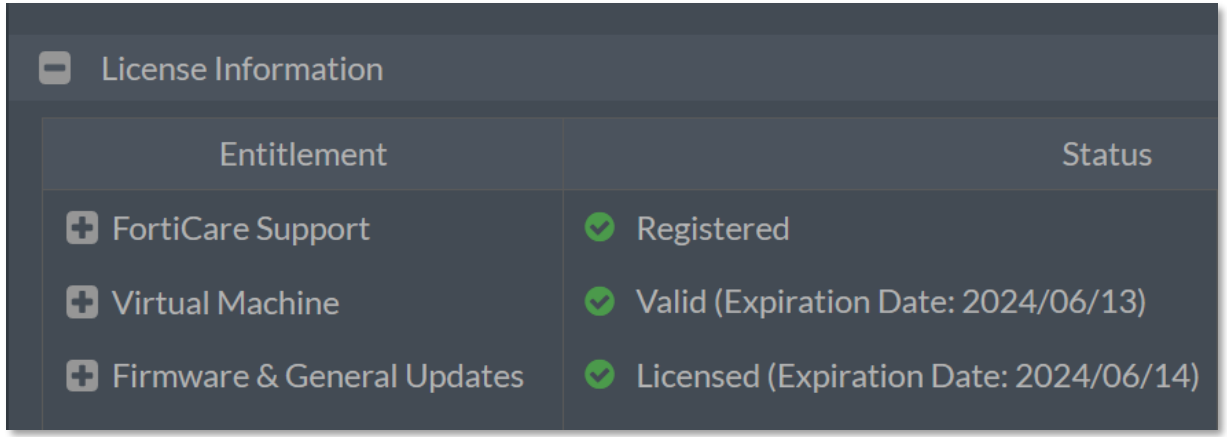
```
config system fortiguard
    set auto-firmware-upgrade {enable | disable}
    set auto-firmware-upgrade-day {sunday monday tuesday wednesday thursday friday saturday}
    set auto-firmware-upgrade-delay <integer>
    set auto-firmware-upgrade-start-hour <integer>
    set auto-firmware-upgrade-end-hour <integer>
end
```

UPDATE MIT INAKTIVEM FORTICARE

- Upgrade ab 7.4.0 auf Major oder Minor Release nur noch mit aktiver FortiCare Lizenz möglich
  - Update im aktuellen Patchpfad wie z.B. **7.4.0** auf **7.4.5** ist möglich
  - Update auf Major Release wie z.B. **7.4.8** auf **7.6.0** ist nicht mehr möglich

- Auch bis anhin darf nur upgedatet werden, wenn eine aktive/gültige FortiCare Lizenz auf dem Gerät vorhanden ist !

Menu: System → FortiGuard




```
diagnose test update info contract
```

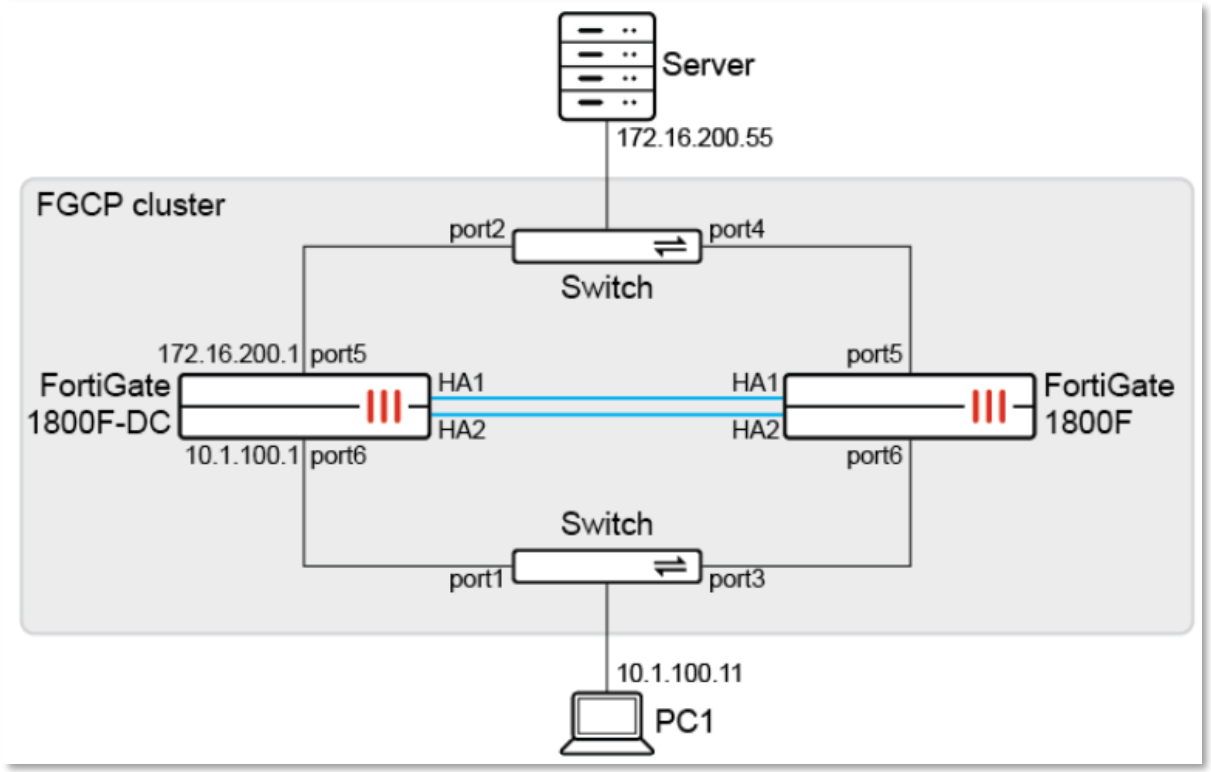
NEUERUNGEN IM HA

FORTIGATE HA MIT DIV AC- UND DC-NETZTEILEN

- Clusterbildung möglich mit dem selben FortiGate Modell aber unterschiedlichen PSUs Setups

- Clusterbedingungen:
  - Gleiches Modell
  - Gleiche Firmware
  - Selbe Hardware Konfiguration (Ausnahme: Netzteil)

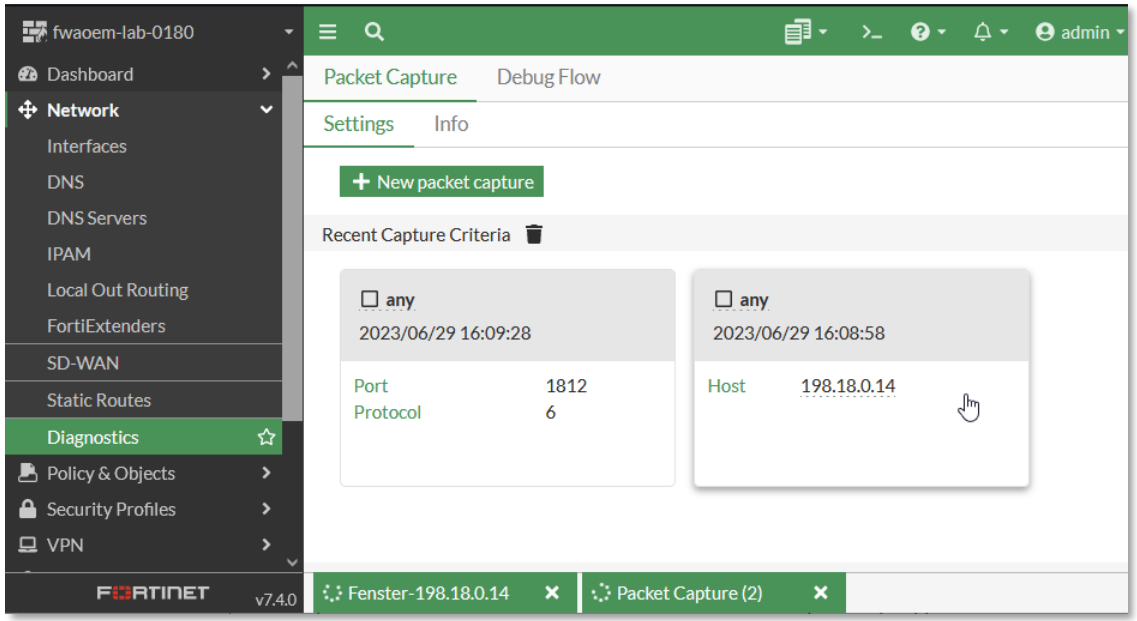
- Beispiel:
  - FortiGate 1800F-**DC** (primär) und FortiGate 1800F (sekundär)



TROUBLESHOOTING PACKET SNIFFER – LIVE

MEHRERE PACKET SNIFFER IM WEBGUI

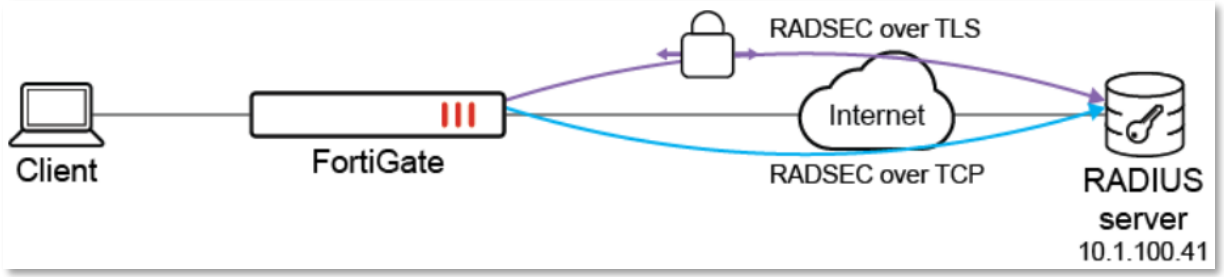
- Es können gleichzeitig mehrere Packet Sniffer Fenster aktiv sein
- Weiteres Navigieren auf der FortiGate möglich (z.B. Policy deaktivieren, und Auswirkung im Sniffer beobachten)
- Fenster können benannt werden



NEUERUNG BEI DER USER AUTHENTIFIZIERUNG

RADSEC CLIENT SUPPORT

- Transport Protokoll
  - UDP: Default UDP (udp1812)
  - TCP: TCP ohne TLS (Auth: tcp1812 Acc: tcp1813)
  - TLS: TLS over TCP (Auth/Acc: tcp2083)

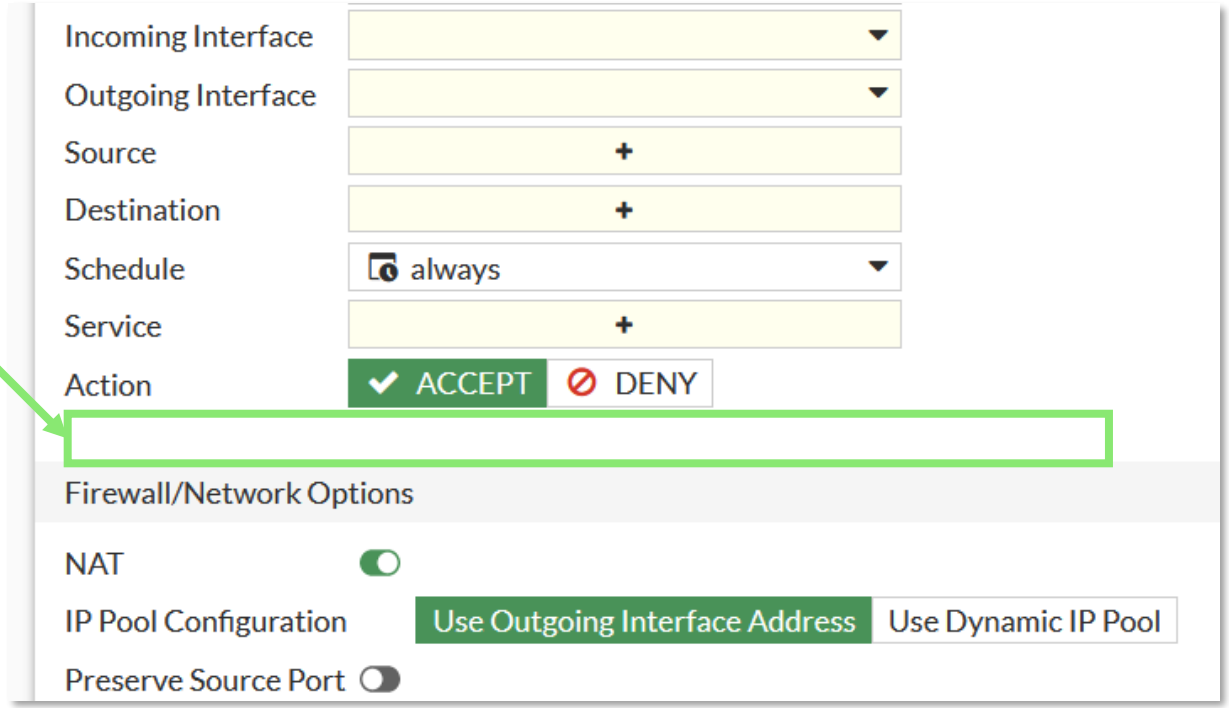



```
config user radius
   edit <name>
       set transport-protocol {udp | tcp | tls}
       set ca-cert <string>
       set client-cert <string>
       set tls-min-proto-version {default | SSLv3 | TLSv1 | TLSv1-1 | TLSv1-2}
       set server-identity-check {enable | disable}
   next
end
```

NEUE FEATURES BEI DEN POLICIES

WO IST DER PROXY MODUS IM WEBGUI?

- Bei kleineren Geräten (<100F) ist nur noch der Flow Modus im WebGUI aktiviert

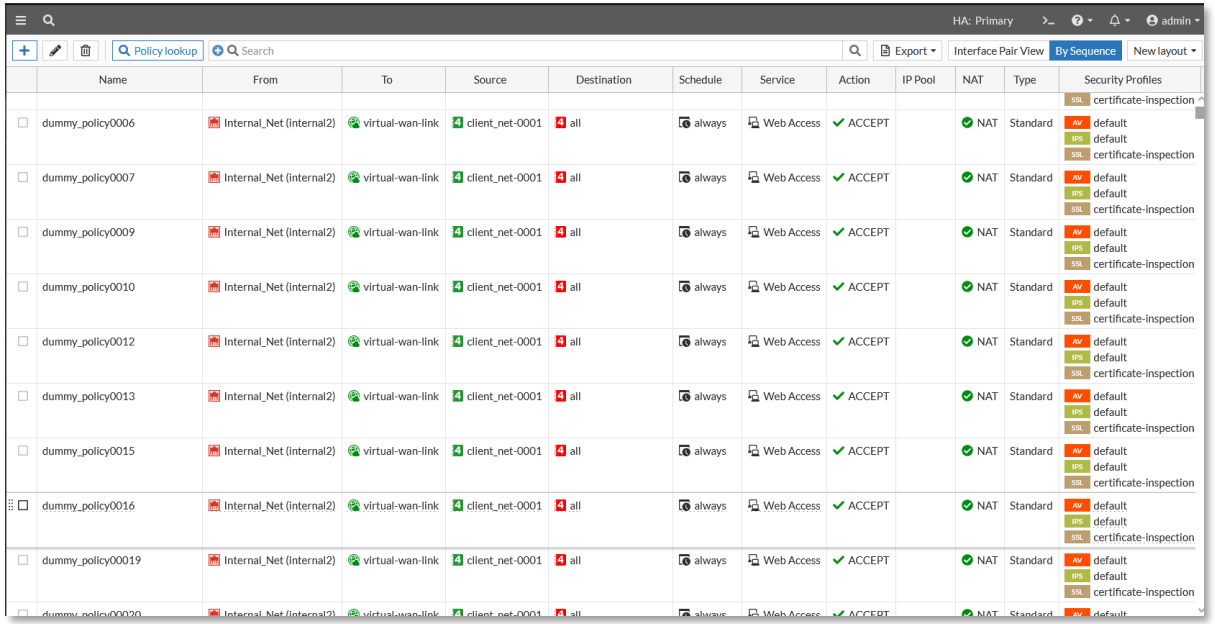


- Über die CLI wieder aktivieren

```
config system setting
      set gui-proxy-inspection enable
end
```

ÜBERARBEITETES POLICY MANAGEMENT

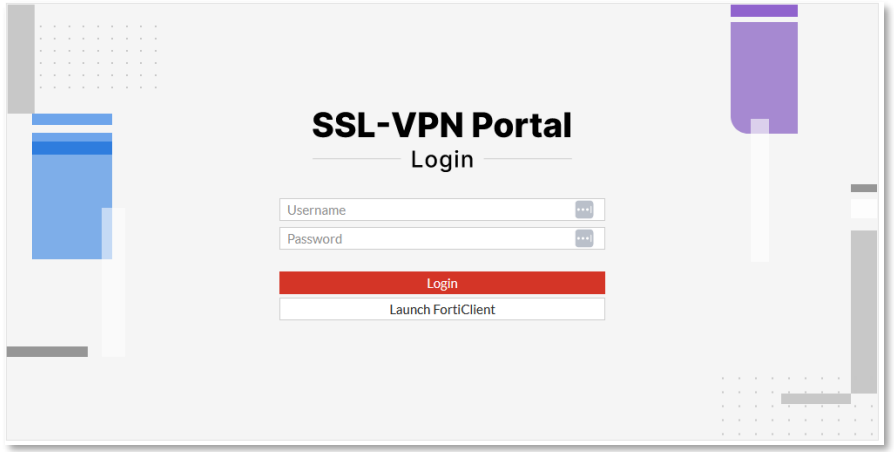
- Auswahl zwischen klassischem und neuem Layout
- Neues Layout:
  - Mehrfach-Selektion möglich
  - Gleichzeitige Änderungen in verschiedenen Regeln möglich (z.B. Source Interface ändern)
  - Für grosse Regelwerke konzipiert
- Es kann jederzeit zwischen den beiden Layouts gewechselt werden

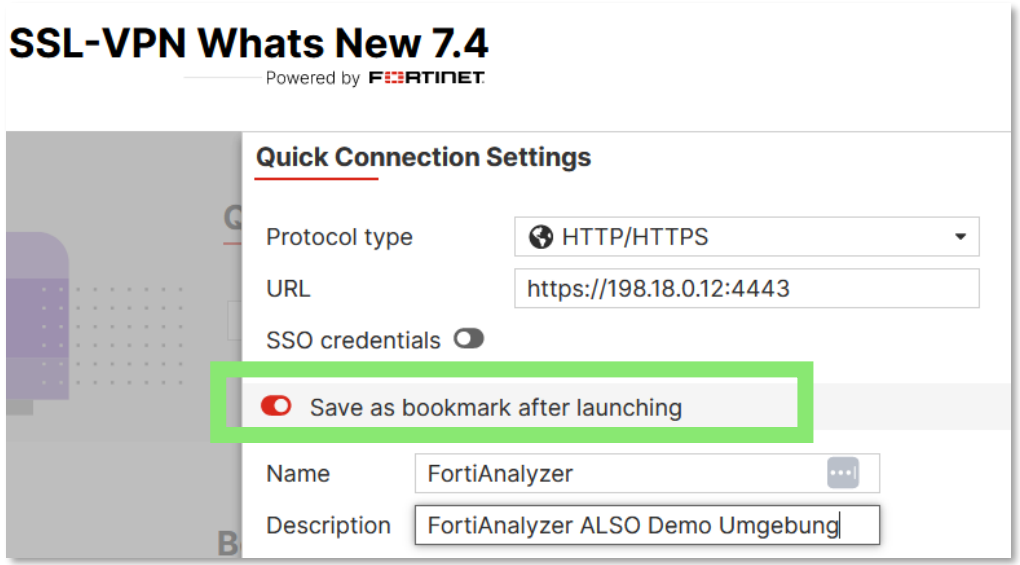


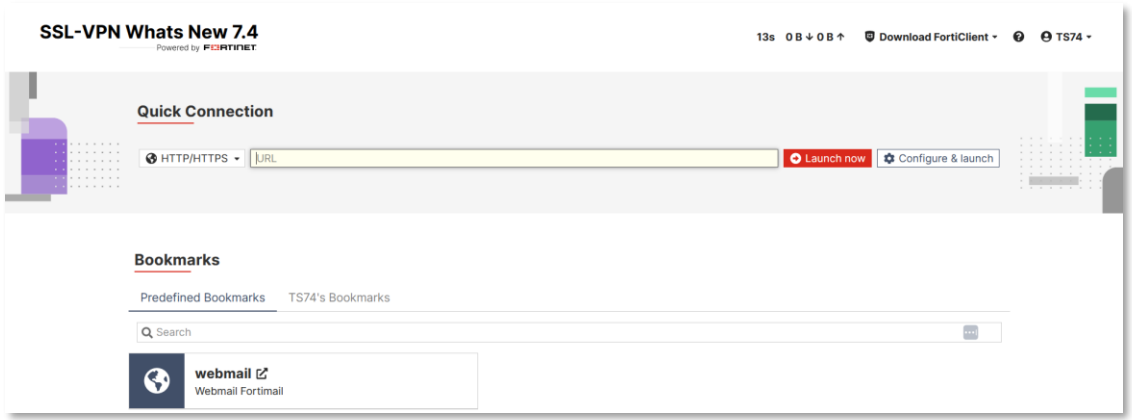
NEUERUNGEN IM SSL-VPN

SSL-VPN LANDINGPAGE ÜBERARBEITET

- Neues Layout auf der Landingpage
- Farbthemen können pro User unabhängig des globalen Farbschemas ausgewählt werden
- Einfache, private Bookmarks können erstellt werden

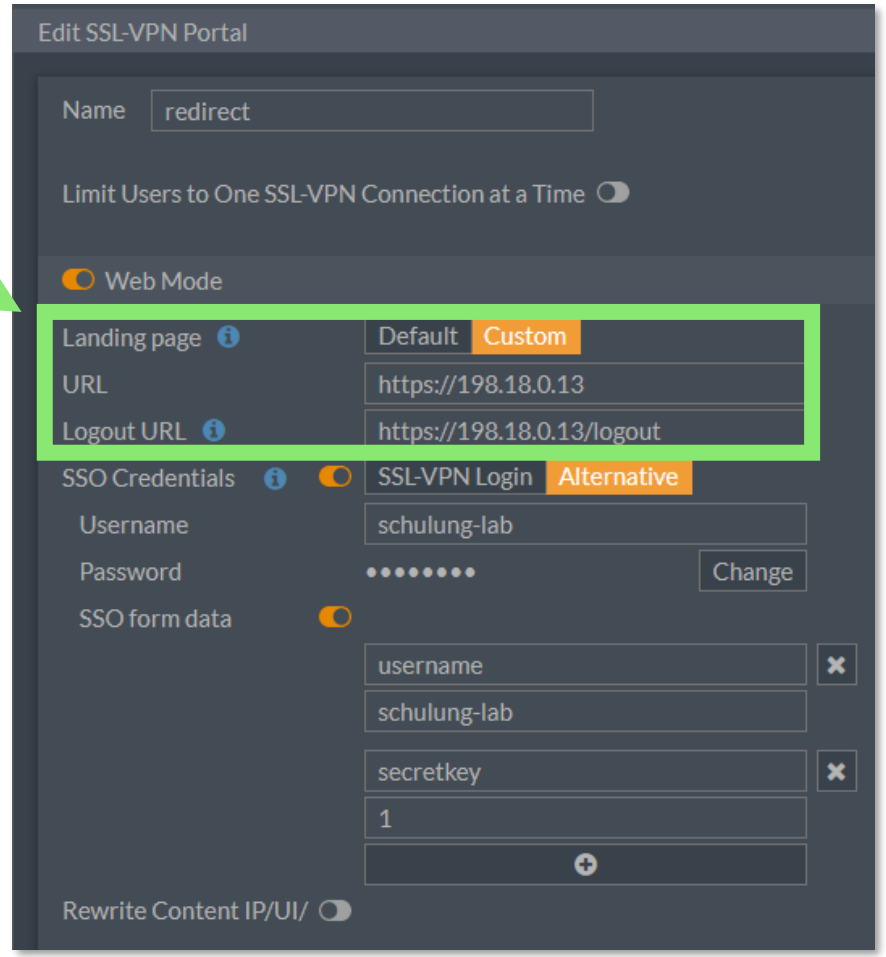






SSL-VPN – REDIRECT AUF EIGENES PORTAL

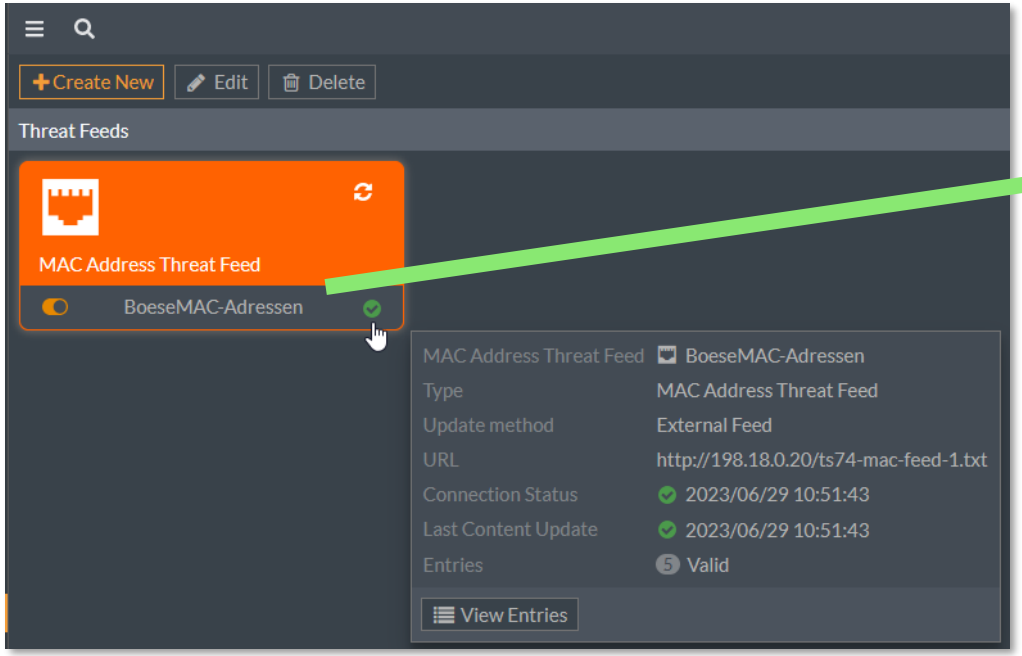
- Es kann auf eigene Landing Page nach dem Authentifizieren geleitet werden

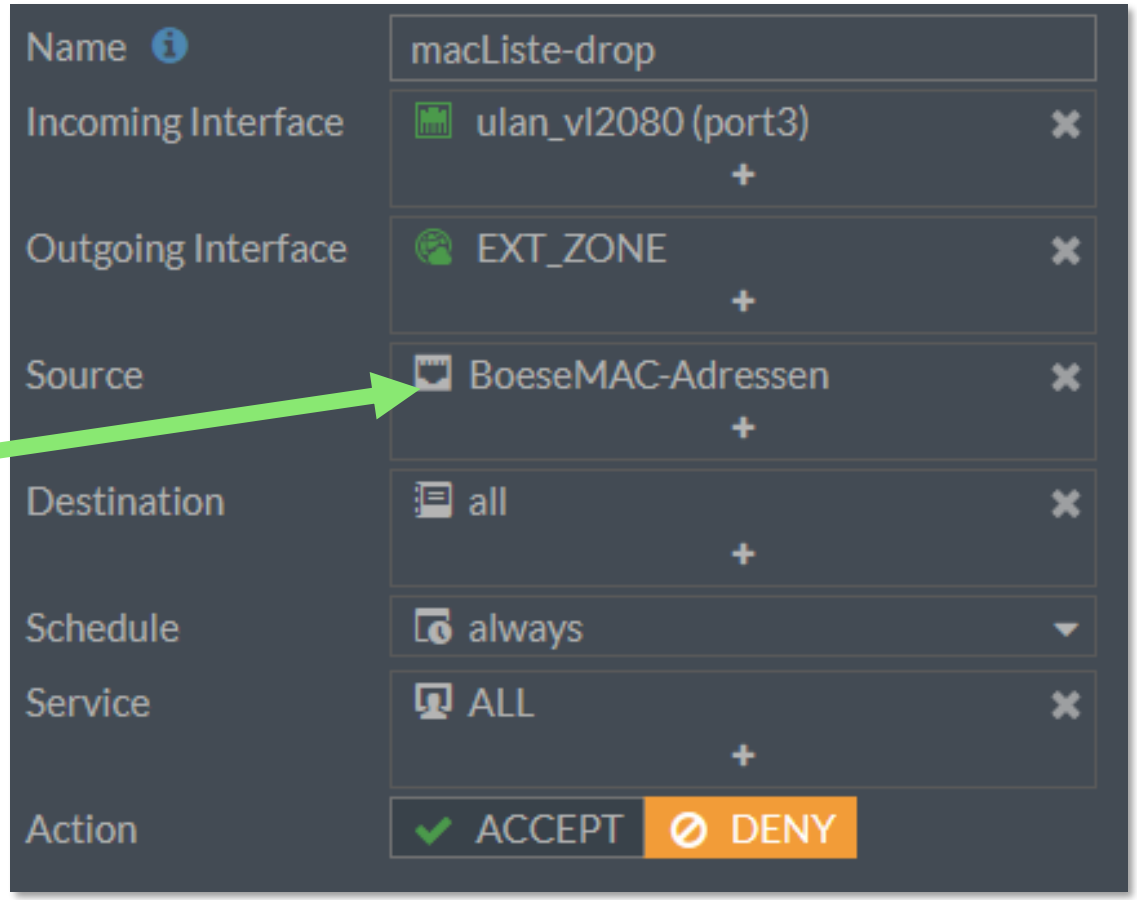


FABRIC SETTING UND KONNEKTOREN – LIVE

MAC FEED – MIT POLICY

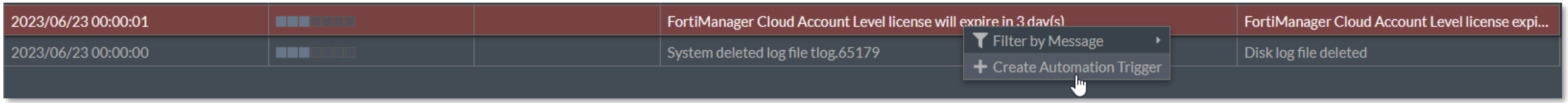
- Externe MAC Adressen Liste wird eingelesen
- Dynamisches Adress Objekt wird erstellt
- Kann in Firewall Regeln als Source/Destination Objekt verwendet werden

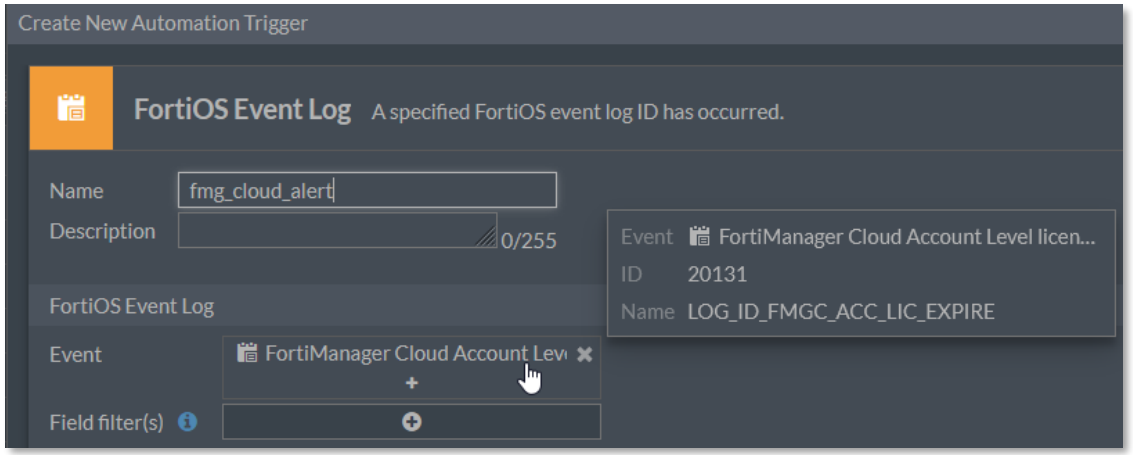




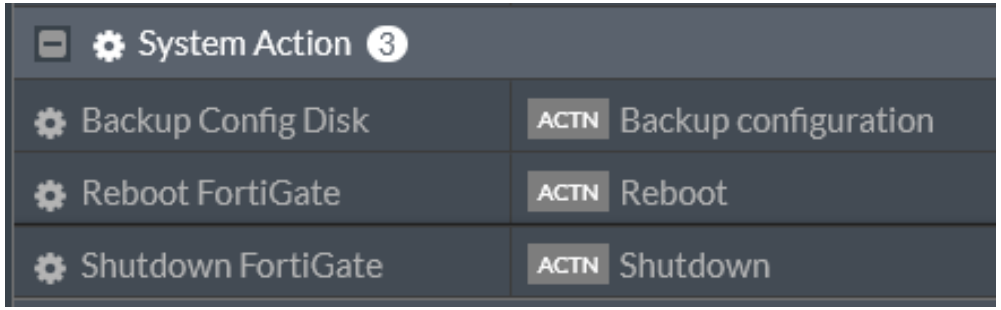
STITCHES DIREKT AUS EVENT LOG ERSTELLEN

- Aus dem Event Log kann direkt ein Trigger konfiguriert werden (erspart mühsames Suchen in der Liste)





- Neue Aktionen:



FORTISWITCH – FEATURES 7.4 UND 7.2.4

FORTISWITCH – SERIENUMMER – ALIAS 7.2.4

- Gewisse Konfigurationen müssen in der CLI der FortiSwitches durchgeführt werden
- In der CLI muss bis anhin mit der Seriennummer auf den entsprechenden Switch verbunden werden
- Neu kann ein Name für den Switch definiert werden, welcher dann in der CLI angesprochen wird

```
config switch-controller managed-switch
rename <SN/NR> to <NAME>
```

POE PORT SETTINGS 7.2.4

- **Port Mode**
  - Strom nach IEEE Standard verteilt (Watt)
  - IEEE802.3 AF = 15W* (12.95W**)
  - IEEE802.3 AT = 30W* (25.5W**)
  - IEEE 802.3BT = 90W* (71.3W**)

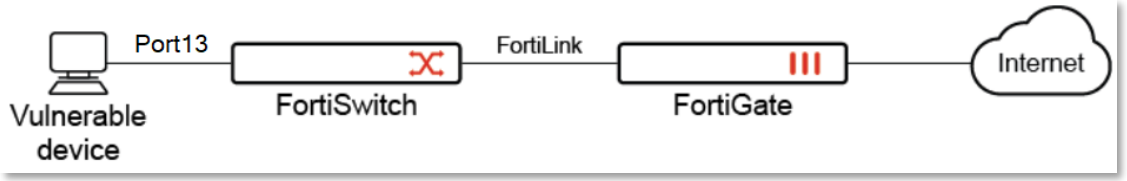
* Ausgangsleistung
** Leistung am Endgerät

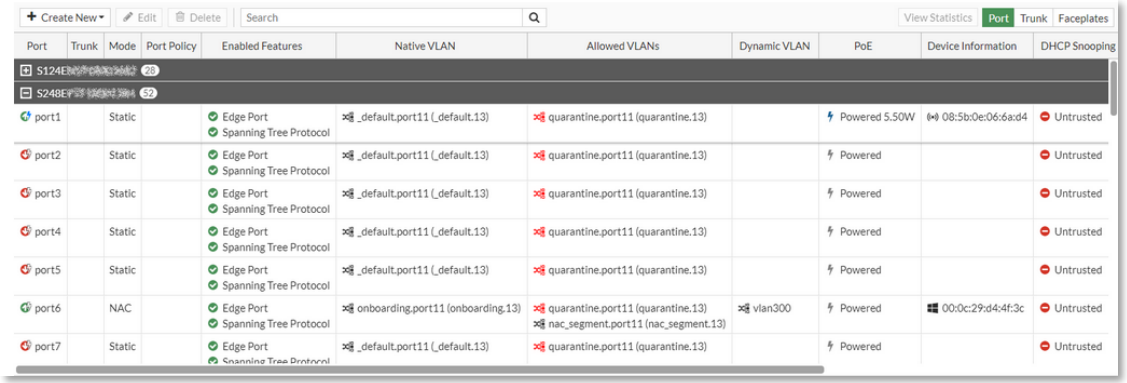
- **Port Priorität**
  - Strom wird nach Priorität verteilt
- **Port Power**
  - Momentan mur auf 1xxE/1xxF Modellen
  - Perpetual: Bei Soft-Reboot noch Strom
  - Perpetual-fast: Bei Hard-Boot noch Strom

```
config switch-controller managed-switch
  edit <FortiSwitch_serial_number>
    config ports
      edit <port_name>
        set poe-port-mode {IEEE802_3AF | IEEE802_3AT | IEEE802.3 BT}
        set mpoe-port-priority {critical-priority | high-priority | low-priority }
        set poe-port-power {normal | perpetual | perpetual-fast}
      next
    end
  next
end
```

OT UND IOT VIRTUAL PATCHING NAC REGELN – 7.4

- Virtuelles OT und IoT Patching anhand von NAC Regeln, welche den Schweregrad der Schwachstelle auf dem Client einstuft, und entsprechende Massnahmen einleitet
- Braucht aktive **IoT Detection Service** Lizenz
- Wenn Kriterien erfüllt, wird das Gerät in ein NAC-VLAN zugewiesen und so isoliert
- Anhand von Firewall Regeln, kann der Zugriff auf das NAC-VLAN ein sicheres Updaten der Geräte ermöglichen.
  - Service Lan → NAC-VLAN Zugriff über https oder tftp um den Patch einzuspielen und das Gerät wieder sicher zu machen

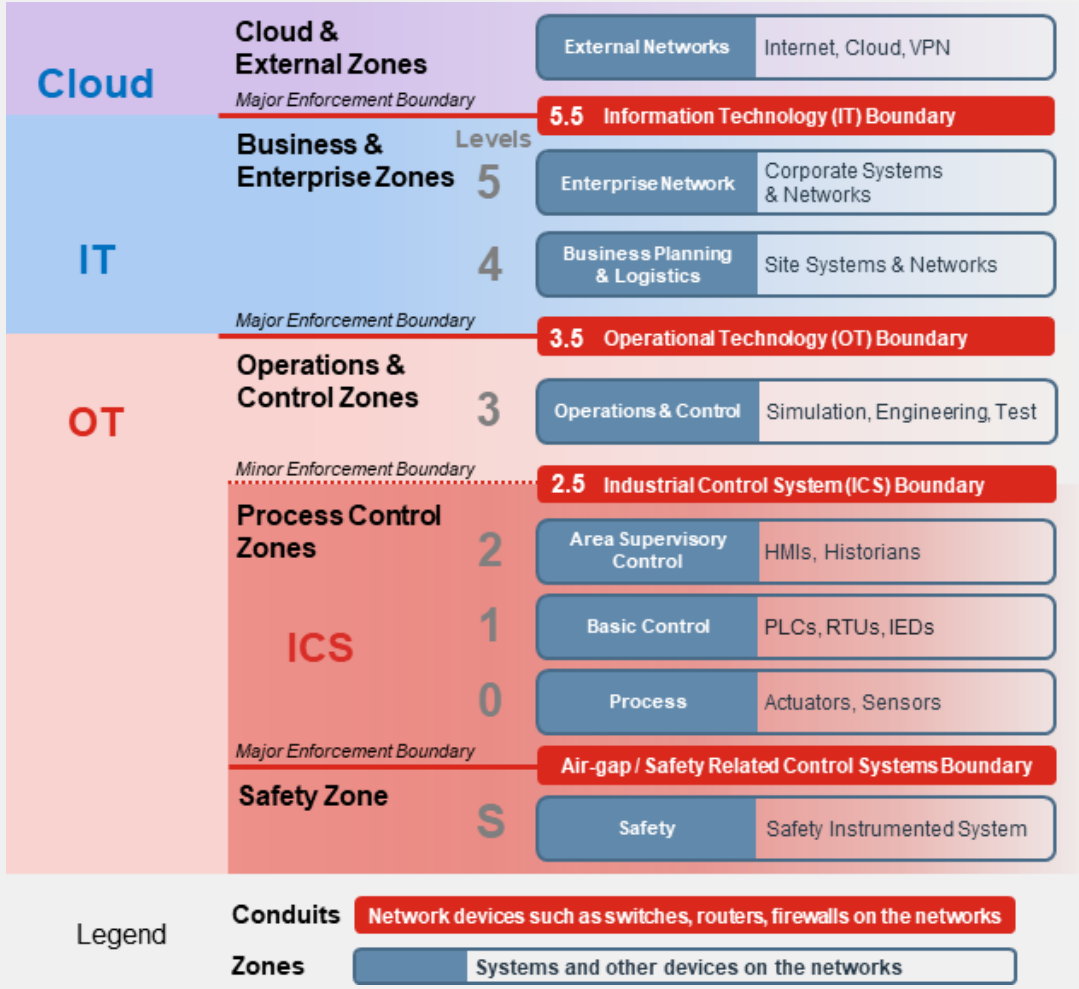




OT Purdue Level View

Purdue Level OT erklärt von CHATGPT

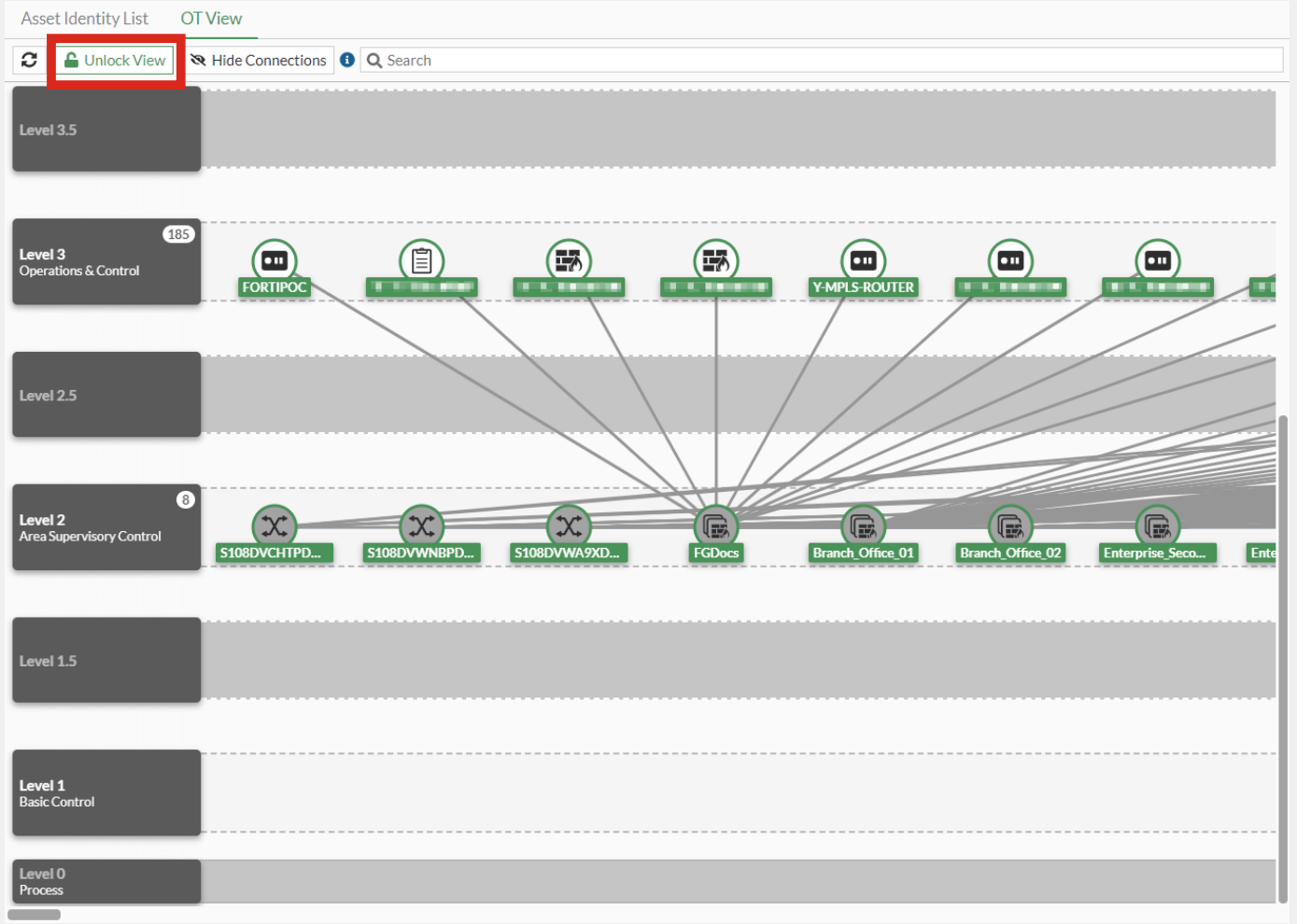
Das Purdue-Modell, auch bekannt als Purdue Enterprise Reference Architecture (PERA), ist ein Sicherheitskonzept für Operationstechnologie (OT). Es teilt OT-Systeme in verschiedene Ebenen oder Zonen auf, um die Sicherheit zu verbessern. Diese Ebenen umfassen die Prozessebene, die Produktionsleitebene, die übergeordnete Leitebene und die Unternehmensebene. Durch die Strukturierung und Trennung der OT-Infrastruktur sollen Sicherheitsrisiken minimiert und Angriffe erschwert werden. Das Purdue-Modell wird in der industriellen Automatisierung und OT-Sicherheit als bewährte Praxis angesehen.



OT Purdue Level View

Security Fabric > Asset Identity Center
Select: *OT View* tab

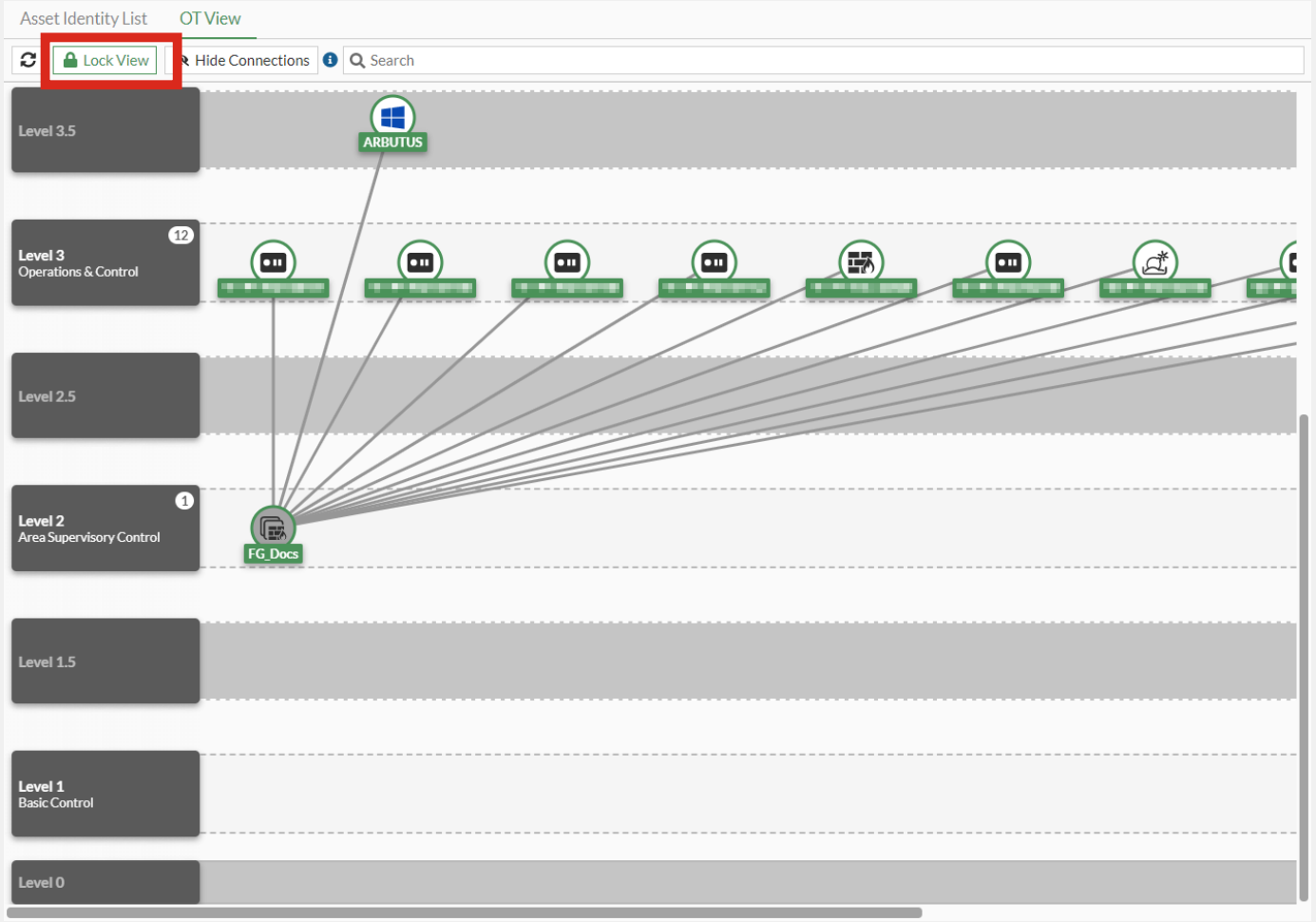
Visualize network assets in Purdue Level based network topology and understand whether the security zones and conduits are implemented correctly and operating as intended.



OT Purdue Level View

Einzelne System anpassen

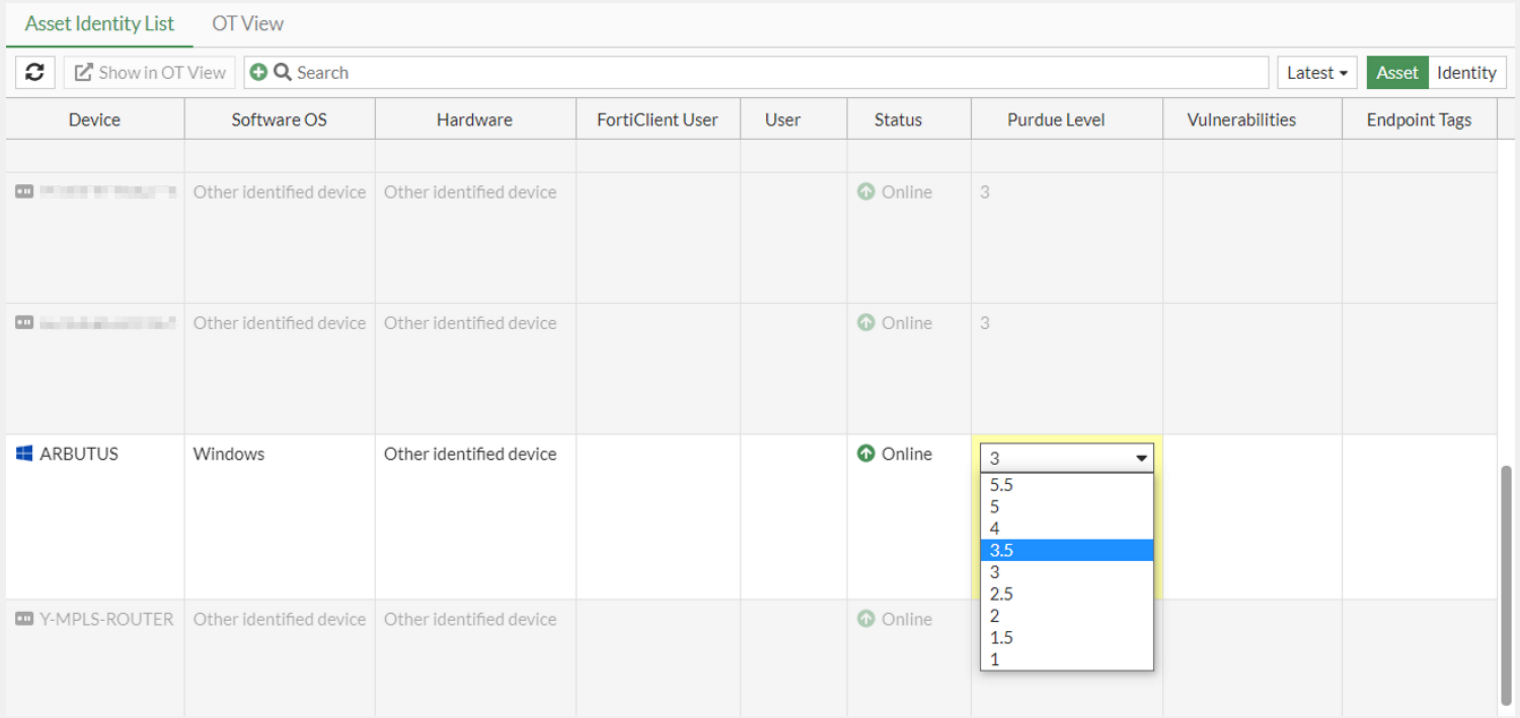
«Drag and Drop» Bearbeitung



OT Purdue Level View

Einzelne Systeme anpassen

Security Fabric > Asset Identity Center



CLI

```
# diagnose user-device-store device memory ot-purdue-set <mac> <ip> <level>
```

`mac`	Enter the MAC address of the device.
`ip`	Enter the IPv4 address of the device.
`level`	Enter the Purdue Level: 1, 1.5, 2, 2.5, 3, 3.5, 4, 5, 5.5.

OT Purdue Level View

Interface Konfigurieren

CLI

Der Default Purdue Level kann mittles CLI auf dem Interface gesetzt werden. (default-purdue-level)
Somit wird automatisch der Default Purdue Level der Systeme gesetzt.
Dieses Feature benötigt eine FortiGuard Industrial Security Service (ISS) Lizenz auf der FortiGate, damit Industrial Database (ISDB) benutzt werden kann. Damit dies funktioniert, muss Device Identification auf dem Interface aktiviert sein.

```
config system interface
  edit <name>
    set device-identification enable
    set default-purdue-level {1 | 1.5| 2 | 2.5| 3 | 3.5 | 4 | 5 | 5.5}
  next
end
```

Default Purdue Level ist 3.
Wenn der Wert auf dem Interface angepasst wird, werden alle Systeme an dem Interface auf den neuen Wert angepasst.
Falls aber schon ein Device gesetzt wurde (GUI oder CLI), wird diese Einstellung preferenziert.

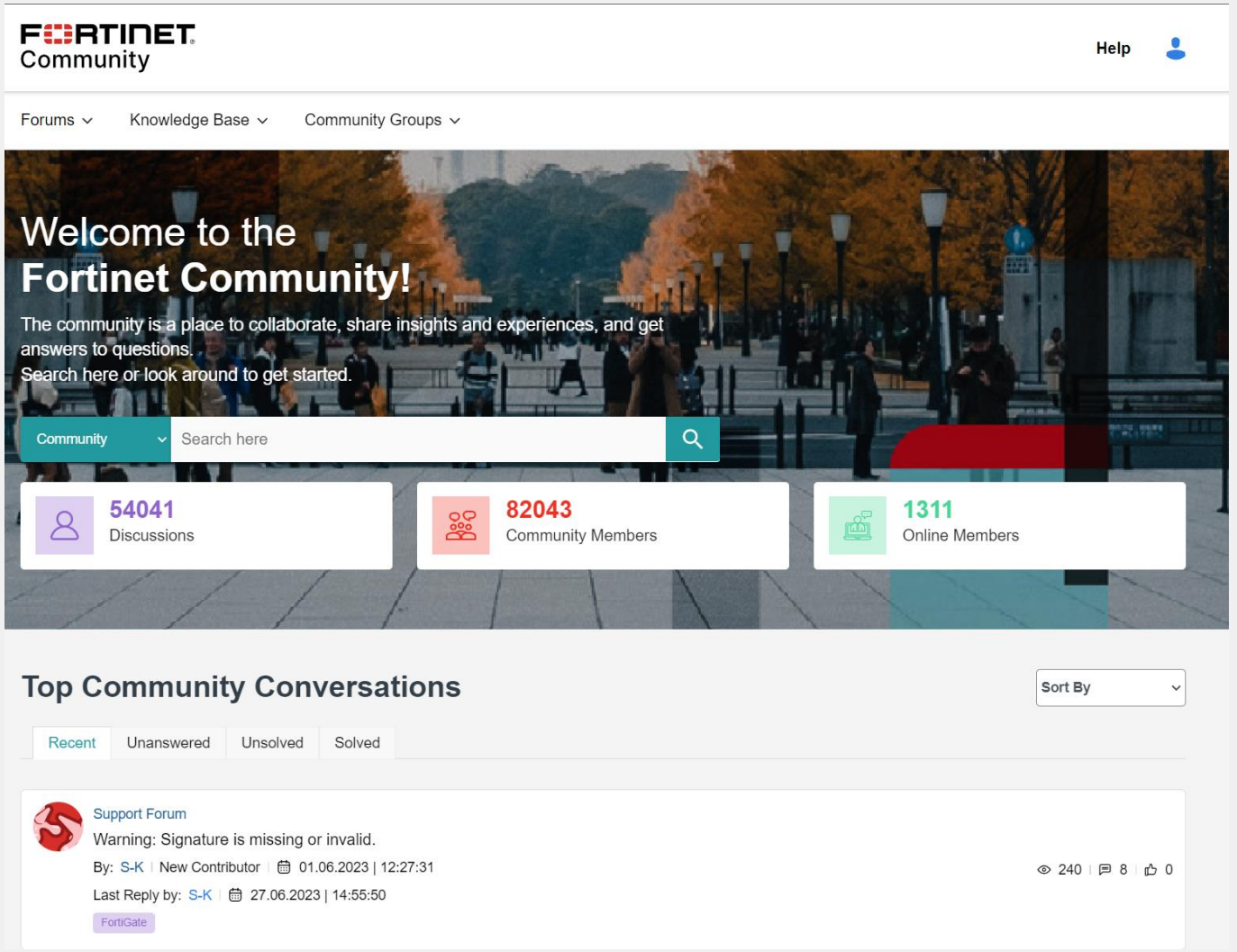
FORTINET COMMUNITY

Fortinet Community
(https://community.fortinet.com)

The community is a place to collaborate, share insights and experiences, and get answers to questions

Requirements:
Only a FortiCloud (free) Account is required to login to the community

FuseCommunity was deprecated and finally replaced by the new community board



AGORA – AGORAWHAT?

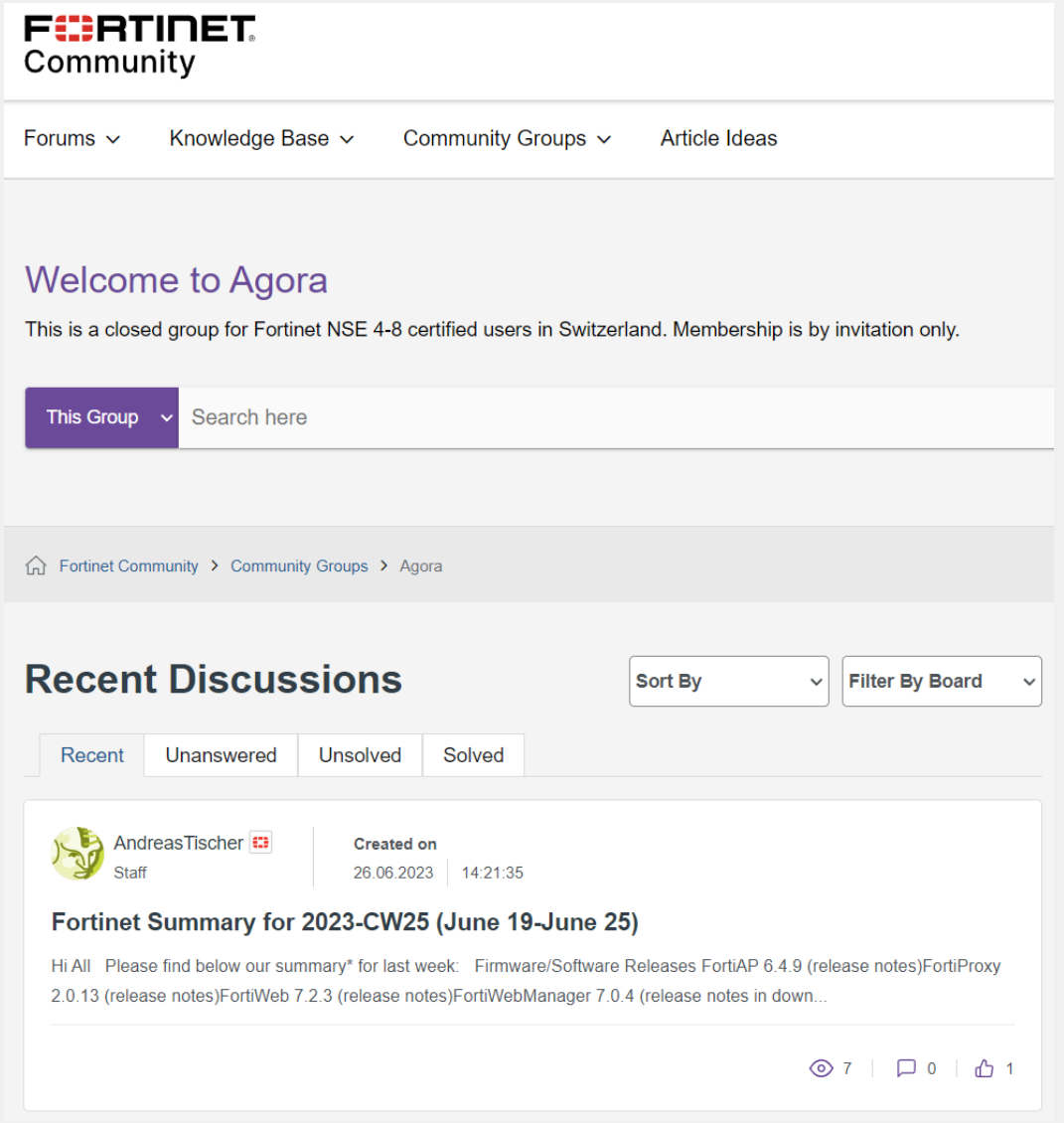
The agora (/ˈægərə/; Ancient Greek: ἀγορά, romanized: agorá, meaning "market" in Modern Greek) was a central public space in ancient Greek city-states. It is the best representation of a city-state's response to accommodate the social and political order of the polis. The literal meaning of the word "agora" is "gathering place" or "assembly". The agora was the center of the athletic, artistic, business, social, spiritual, and political life in the city. The Ancient Agora of Athens is the best-known example.

AGORA – Where and what to find…

https://community.fortinet.com/t5/Agora/cmp-p/grouphub:agora

→ Login → Community Groups → Local Groups → AGORA

- Weekly Tech Update Newsletter for FTNT Employees, NSE4-certified Partners and Distribution
- Planned Release: every Monday – Tuesday
- Content: SW & HW Releases, newly and updated KBs, Videos, Soundcloud Content, EOS - EOL - EOO Information, Threat Information, Blogs, planned Events, Event-recordings, Product Specification Updates and more…
- Monthly Product Guide and HW Schematics Uuploads with „handmade“ Change Logs (Yes, it‘s crazy but they like it)



FRAGT UNS… ???

Unsere Email : security-ch@also.com

Unser Wiki: https://fortinet.also.ch/wiki

THANK YOU